VISA GLOBAL COMPROMISED ACCOUNT RECOVERY PROGRAM

VISA

WHAT EVERY MERCHANT SHOULD KNOW ABOUT GCAR

WHAT EVERY MERCHANT SHOULD KNOW ABOUT GCAR

WHAT

The Visa Global Compromised Account Recovery (GCAR) program offers a balanced, simplified, and cost-effective recovery process for Visa clients worldwide. The program enables issuers to recover a portion of costs associated with counterfeit magnetic-stripe losses and/or PIN data fraud losses, as well as a portion of the associated operating expenses, for qualified account data compromise events. The program also limits liability of merchant banks for fraud costs associated with a data compromise event to a maximum window of time and further caps losses associated with operating expenses and catastrophic liability losses.

GCAR covers VisaNet card present point-of-sale (POS) and VisaNet ATM losses across all Visa-owned brands where it is determined that a violation of the Payment Card Industry Data Security Standard (PCI DSS), PIN Management Requirements Documents, or the *PIN Security Program Guide* could have allowed an account data compromise and subsequent financial loss. Under GCAR, financial losses may be associated with Visa transactions (including Visa Electron transactions), Interlink transactions or Plus transactions.

WHY

Account data compromises resulting from non-PCI DSS-compliant data security can have an adverse impact on the Visa payment system and result in losses and additional expenses for issuers whose cardholder accounts are at risk. Having fair and predictable rules that allocate responsibility for the financial impact of an account data compromise is important for all stakeholders in the Visa payment system.

WHEN

The GCAR program went into effect on May 15, 2012, replacing the US Account Data Compromise Recovery (ADCR), Canadian Data Compromise Recovery Solution (DCRS) and DCRS International programs. If an event had at least one Internet Compromise (IC) and/or Research & Analysis (RA) Compromised Account Management System (CAMS) alert sent on or after May 15, 2012, any assessment will be calculated under the GCAR program.

WHO

The program is limited to compromises at merchants, acquirers, acquirer processors, data aggregation points, service providers, and/or agents.

HOW

The following describes how the GCAR process works.

ACCOUNT COMPROMISE AND SUBSEQUENT COUNTERFEIT FRAUD

Criminals exploit a system or operational vulnerability to access Merchant A's point-of-sale (POS) system with PIN and/or full magnetic-stripe card data. Valid account information is at risk, some or all of which may be accessed by the criminals.

The stolen account information may be downloaded to a computer, and/or encoded on counterfeit cards or re-encoded on lost/stolen cards.

Card issuers approve transactions resulting from the counterfeit cards (with seemingly valid data) since no lost/stolen card or fraud on that account number has been reported at this point.

COMPROMISED ACCOUNT MANAGEMENT SYSTEM (CAMS)

A suspected or confirmed data compromise of a merchant or processor is reported to Visa, either through a self-report by the compromised entity or based on issuer submitted reports on a common point of purchase or processing.

A PCI Forensic Investigation (PFI) is conducted to validate a data breach and determine if any accounts are at risk. If so, Visa sends an alert via CAMS to issuers with compromised accounts.

GCAR PROCESS

Visa determines if the account compromise potentially meets the GCAR Event Qualification Criteria. (See next page for details)

A reasonable time after completion of the PCI Forensic Investigation (PFI), Visa will notify the sponsor merchant acquirer bank of the potential GCAR qualification.

At the end of the issuer fraud reporting/chargeback window (CAMS date plus 125 days), Visa determines if an event qualifies under GCAR. If the event qualifies, Visa calculates the acquirer liability and issuer recovery. Visa then notifies the acquirer of the amount and qualification details. The acquirer may exercise appeal rights by submitting any appeal documents with new information relevant to the assessment within 30 days of receipt of the qualification summary.

Acquirers are debited approximately 30 calendar days after notification or the completion of the appeal process. Issuers are credited approximately 30 calendar days after Visa has collected the funds from the responsible acquirers.

GCAR provides a defined window of financial exposure associated with each event CAMS alert. The dates of first exposure and containment of the breach will determine the Fraud Window assigned to each alert. If an event involves multiple CAMS alerts, each alert may have a different Fraud Window. The Fraud Window can extend up to 12 months prior to and one month past the date of each IC/RA CAMS alert. Counterfeit fraud transactions must occur within the Fraud Window for one or more event alerts to be eligible for GCAR.

GCAR EVENT QUALIFICATION CRITERIA

To qualify an Account Data Compromise event under the GCAR program, Visa must determine all of the following criteria have been met:

1. A PCI DSS or PCI PIN Security or PIN Security Program Guide violation has occurred that could have allowed a compromise of Primary Account Number (PAN) and Card Verification Value (CVV) magnetic-stripe data and/or PIN data.
2. Primary Account Number (PAN) and Card Verification Value (CVV) magnetic-stripe data, and/or PIN data, is exposed at the compromised entity during the Intrusion Access Window.
3. 15,000 or more eligible accounts were sent in one or more CAMS IC or RA alerts and/or Visa Account Bulletin (VAB) alerts indicating Primary Account Number (PAN) and Card Verification Value (CVV) magnetic-stripe data is potentially at risk.
4. A combined total of US $150,000 or more recovery for all issuers involved in the event.
5. Elevated magnetic-stripe counterfeit fraud was observed in the population of eligible accounts sent in the CAMS alert(s) associated with the Account Data Compromise Event.

GCAR RECOVERY CALCULATION RULES

Under the GCAR program, Visa uses a basic set of rules to calculate an acquirer's liability for issuer incremental counterfeit fraud losses and a pre-determined amount to cover operating expenses associated with accounts at risk in the compromise event. These calculations are based on eligible CAMS-alerted accounts and issuer-reported counterfeit fraud that occurred during the alert Fraud Window for one or more event alerts.

Visa also may impose a liability cap for compromises that meet specified criteria to be deemed catastrophic, based on a balancing of the overall interests of the system. For merchant compromises where other criteria are met, the cap on the acquirer's liability is calculated based on the annual Visa sales volume of transactions submitted by acquirers for entities owned or controlled by the legal owner of the compromised entity. This will include Visa sales at all entities owned by the legal owner of the compromised entity.

Visa CAMS offers a secure and efficient way for acquirers and law enforcement agencies to upload potentially compromised and recovered accounts to Visa through a secure site. Once account files are received, CAMS processes then distributes the alerts to subscribing financial institutions via e-mail.

REDUCE LOSSES AND RISK FROM A COMPROMISE

Non-PCI-Compliant entities storing magnetic-stripe and/or PIN data provide criminals with an attractive and vulnerable platform from which to steal sensitive cardholder information. As the very nature of magnetic-stripe and PIN data theft continues to evolve, so does the need for merchants to proactively strengthen their security controls and greatly reduce their exposure to account compromise risk.[1]

TO AVOID DATA STORAGE VIOLATIONS:

- **Be PCI DSS-compliant.** Contact your merchant bank to understand roles and respective obligations to validate and maintain PCI DSS compliance. For more information about the PCI DSS and the PCI PIN security requirements, visit www.pcisecuritystandards.org.
- **Do not store magnetic-stripe data or PIN blocks after transaction authorization.** The full contents of track data, which is read from the magnetic-stripe or PIN, which is entered by the cardholder, must not be retained on any system after a transaction is authorized. The personal account number (PAN), expiration date, and customer name may be retained as long as it is protected in accordance with the PCI DSS.
- **Evaluate your payment application.** Ensure the payment application you are using is Payment Application Data Security Standard (PA-DSS) compliant. A list of PA-DSS Validated Payment Applications can be found at the PCI Security Standards Council's (SSC) website at www.pcisecuritystandards.org.
- **Immediately report an account compromise.** If you suspect an account compromise, alert all necessary parties of a suspected or confirmed security breach immediately. Provide all compromised Visa account numbers to your merchant bank within 24 hours.

SOME GCAR TERMS IN BRIEF

For more information
To learn more about the GCAR program and/or PCI DSS requirements, please contact your merchant bank.

Event CAMS Date	The final alert sent in a multi-alert compromise event. In single alert events, the CAMS Date will be the same as the date of the single alert.
Fraud Window	A 13-month maximum time period that can be up to 12 months prior to and one month past the alert CAMS Date. Counterfeit fraud transactions must fall within the Fraud Window to qualify for recovery. If an event involves multiple CAMS alerts, each alert may have a different Fraud Window. The Fraud Window cannot begin before the start of an event's Intrusion Access Window.
Intrusion Access Window	A period of time during which data was improperly accessed as a result of a data compromise event and could have been stolen.
IC CAMS Alert	IC is a source indicator for the exposed accounts that are being provided in the CAMS notification. IC stands for Internet, network or system-related compromise.
RA CAMS Alert	RA is a source indicator for exposed accounts that are being provided in the CAMS notification. RA stands for Research and Analysis (i.e., skimming, POS or ATM tampering; lost or stolen data not associated with a computer intrusion).
PA CAMS Alert	PA is a source indicator for exposed accounts that are part of an incident that is unconfirmed and the forensic investigation has not been completed. These accounts are being provided as an early warning and will not be eligible for the Global Compromised Account Recovery (GCAR).

[1] To protect all parties to the Visa system, participants with access to personal Visa account information or Visa transaction information are responsible for following rigorous standards for data protection set by Visa. These standards may be consistent with or exceed industry standards. For example, the storage of magnetic-stripe data is strictly prohibited. *Visa International Operating Regulations (VIOR)* ID#: 010410-010410-0007815 (15 April 2013).